Patent claims

1. A data carrier with a semiconductor chip (5) having at least one memory in which an operating program containing a plurality of commands is stored, each command causing signals detectable from outside the semiconductor chip (5), characterized in that the data carrier (1) is designed to perform security-relevant operations solely executing operating program commands of such a kind, or executing said commands in such a way, that the data processed with the corresponding commands cannot be inferred from the detected signals.
2. A data carrier according to claim 1, characterized in that the commands used are designed for at least byte-by-byte processing of data.
3. A data carrier according to ~~either of the above claims~~ claim 1, characterized in that the commands used are indistinguishable with respect to the signal patterns caused thereby.
4. A data carrier according to ~~any of the above claims~~ claim 1, characterized in that the commands used each lead to a signal pattern which is substantially independent of the data processed with the command.
5. A data carrier according to ~~any of the above claims~~ claim 1, characterized in that the operating program is able to execute a series of operations (f), input data being required for executing the operations (f) and output data being generated by execution of the operations (f), whereby
   - the input data are falsified by combination with auxiliary data (Z) before execution of one or more operations (f),
   - the output data determined by execution of the one or more operations (f) are combined with an auxiliary function value ($f(Z)$) in order to compensate the falsification of the input data,
   - whereby the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored on the data carrier (1) along with the auxiliary data (Z).

6. A data carrier according to claim 5, characterized in that the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is non-linear with respect to the combination generating the falsification.

7. A data carrier according to ~~either of claims 5 and 6~~ claim 5, characterized in that the auxiliary data (Z) are varied, the corresponding auxiliary function values ($f(Z)$) being stored in the memory of the data carrier (1).

8. A data carrier according to claim 7, characterized in that new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combining two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).

9. A data carrier according to claim 8, characterized in that the existing auxiliary data (Z) and auxiliary function values ($f(Z)$) intended for the combination are each selected randomly.

10. A data carrier according to ~~any of claims 5 to 7~~ claim 5, characterized in that pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).

11. A data carrier according to ~~any of claims 5 to 10~~ claim 5, characterized in that the auxiliary data (Z) are a random number.

12. A data carrier according to ~~any of claims 5 to 11~~ claim 5, characterized in that the combination is an EXOR operation.

13. A data carrier according to ~~any of the above claims~~ claim 1, characterized in that a plurality of operations can be executed with the operating program, it holding for at least a subset of said operations that the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and the order of execution of the stated subset of operations is varied at least when the subset contains one or more security-relevant operations.

14. A data carrier according to claim 13, characterized in that the order of execution is varied at each run through the stated subset of operations.

15. A data carrier according to claim 13 ~~or 14~~, characterized in that the order of execution is varied according to a fixed principle.

ART 34 AMDT

16. A data carrier according to claim 13 ~~or 14~~, characterized in that the order of execution is varied randomly.

17. A data carrier according to ~~either of claims 13 and 14~~ claims 13, characterized in that the order of execution is varied in accordance with the data processed with the operations (*f*).

18. A data carrier according to ~~any of claims 13 to 17~~ claim 13, characterized in that the order of execution is fixed before execution of the first operation (*f*) of the subset for all operations of the subset whose execution is intended to be directly successive.

19. A data carrier according to ~~any of claims 13 to 18~~ claim 13, characterized in that it is fixed before the onset of execution of an operation (*f*) of the subset which operation of the subset whose execution is intended to be successive is executed next.

20. A data carrier according to ~~any of the above claims~~ claim 1, characterized in that the security-relevant operations are key permutations or permutations of other secret data.

21. A data carrier according to ~~any of the above claims~~ claim 1, characterized in that the data carrier is a smart card.

22. A method for executing security-relevant operations in a data carrier (1) with a semiconductor chip (5) having at least one memory in which an operating program containing a plurality of commands is stored, each command causing signals detectable from outside the semiconductor chip (5), characterized in that the data carrier performs security-relevant operations (*f*) solely using operating program commands of such a kind, or using said commands in such a way, that the data processed with the corresponding commands cannot be inferred from the detected signals.

23. A method according to claim 22, characterized in that the commands used employ data present at least byte by byte.

24. A method according to ~~either of claims 22 and 23~~ claim 22, characterized in that the commands used are indistinguishable with respect to the signal patterns caused thereby.

ART 34 AMDT

25. A method according to ~~any of claims 22 to 24~~ claim 22, characterized in that the commands used each lead to a signal pattern which is substantially independent of the data processed with the command.

26. A method for protecting secret data serving as input data for one or more operations, characterized in that

- the input data are falsified by combination with auxiliary data (Z) before execution of the one or more operations (f),
- the output data determined by execution of the one or more operations (f) are combined with an auxiliary function value ($f(Z)$) in order to compensate the falsification of the input data,
- whereby the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored along with the auxiliary data (Z).

27. A method according to claim 26, characterized in that the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is nonlinear with respect to the compensation generating the falsification.

28. A method according to ~~either of claims 26 and 27~~ claim 26, characterized in that the auxiliary data (Z) are varied, the corresponding auxiliary function values ($f(Z)$) being stored in the memory of the data carrier.

29. A method according to claim 28, characterized in that new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combination of two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).

30. A method according to claim 29, characterized in that the existing auxiliary data (Z) and auxiliary function values ($f(Z)$) intended for the combination are each selected randomly.

31. A method according to ~~any of claims 26 to 30~~ claim 26, characterized in that pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).

ART 34 AMDT

32. A method according to ~~any of claims 26 to 31~~ claim 26, characterized in that the auxiliary data (Z) are a random number.

33. A method according to ~~any of claims 26 to 32~~ claim 26, characterized in that the combination is an EXOR operation.

34. A method for executing a plurality of operations (f) within the operating system of a data carrier (1), it holding for at least a subset of said operations that the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and the order of execution of the stated subset of operations is varied at least when the subset contains one or more security-relevant operations.

35. A method according to claim 34, characterized in that the order of execution is varied at each run through the stated subset of operations.

36. A method according to claim 34 ~~or 35;~~ characterized in that the order of execution is varied according to a fixed principle.

37. A method according to claim 34 ~~or 35;~~ characterized in that the order of execution is varied randomly.

38. A method according to ~~either of claims 34 and 35~~ claim 34, characterized in that the order of execution is varied in accordance with the data processed with the operations (f).

39. A method according to ~~any of claims 34 to 38~~ claim 34, characterized in that the order of execution is fixed before execution of the first operation of the subset for all operations of the subset.

40. A method according to ~~any of claims 35 to 39~~ claim 35, characterized in that it is fixed before the onset of execution of an operation (f) of the subset which operation of the subset whose execution is intended to be successive is executed next.

41. A method according to ~~any of claims 22 to 40~~ claim 22, characterized in that the security-relevant operations are key permutations or permutations of other secret data.